REMARKS

In an Office Action dated September 17, 2010, claims 1-14 and 17-37 were rejected. Applicants respectfully request reconsideration of the present application based on the following remarks.

I. Claim Rejections under 35 U.S.C. 103

Claims 1-14, and 17-37 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffstein et al. (US 6,298,137, hereafter "Hoffstein") in view of Irvin (US 6,832,314). Applicants respectfully request reconsideration of the above-noted rejection in view of the following.

Claim 1 recites: that error condition information is a conditional expression indicating a condition for causing no decryption error; that the conditional expression is represented as $2 \cdot p \cdot d + 2df - 1 < q/2$, with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non-negative integer df; and that the non-negative integer df specifies a number of coefficients in a private key polynomial f whose coefficient values equal to 1. Applicants respectfully submit that the above-noted features of claim 1 are not disclosed, suggested, or otherwise rendered obvious by any combination of Hoffstein and Irvin.

Applicants note that in the "Response to Arguments" section on pages 2 and 3 of the Office Action, the Examiner appears to take the position that the error conditional information of claim 1 is suggested by Cols. 6-12 of Hoffstein in view of the disclosure of a "fifth type of trap-door function" at Col. 2, Lines 14-21. Additionally, Applicants note that in the rejection of claim 1 on pages 4-6 of the Office Action, the Examiner appears to take the position that the error conditional information of claim 1 corresponds to Col. 9, Lines 44-67, Col. 10, Lines 25-52, and Col. 11, Lines 10-55. Applicants respectfully disagree.

In this regard, Hoffstein is directed to a ring-based public key cryptosystem method. Applicants note that Cols. 6-12 describe an embodiment of the public key cryptosystem using an example of message transmission between a sender, Cathy, and a receiver, Dan. Applicants note that the example merely discloses encoding an M x M matrix based upon random integers which

fulfill a predetermined condition (*See* Col. 9, Lines 44-67).

However, Applicants note that the above-noted sections of Hoffstein cited by the Examiner fail to teach the use of a conditional expression $2 \cdot p \cdot d + 2df - 1 < q/2$ for indicating that no error has occurred, as required by claim 1.

Further, Applicants note that within the conditional expression required by claim 1, the parameter "df" is used to specify the number of coefficients in a private key polynomial f whose coefficient values are equal to 1. Applicants note that Hoffstein contains no disclosure corresponding to the parameter "df." As such, Applicants respectfully submit that because Hoffstein contains no disclosure corresponding to the parameter "df" as defined by claim 1, Hoffstein necessarily fails to teach the conditional expression $2 \cdot p \cdot d + 2df - 1 < q/2$, as required by claim 1.

Irvin is directed to a method of selective encryption and decryption over a communication network based on one or more provided encryption keys (Abstract). Applicants note that while Irvin discloses that an error check value based on an encrypted message may be generated, Irvin fails to disclose error conditional information being a conditional expression represented as $2 \cdot p \cdot d + 2df - 1 < q/2$, in which the parameter "df" specifies the number of coefficients in a private key polynomial f whose coefficient values are equal to 1, as required by claim 1.

In view of the above, Applicants respectfully submit that any combination of Hoffstein and Irvin fail to disclose, suggest, or otherwise render obvious the above-noted features of claim 1. Therefore, claim 1 is patentable over any combination of Hoffstein and Irvin.

Additionally, Applicants respectfully request that, if the rejection of claim 1 is maintained, the Examiner explicitly inform Applicants of the locations in the disclosure of the cited references that correspond to the conditional expression $2 \cdot p \cdot d + 2df - 1 < q/2$ and the parameter "df," such that Applicants may readily judge the prospects of an appeal.

Claims 2-14 and 17 are patentable over any combination of Hoffstein and Irvin based at least on their dependency from claim 1.

Claims 18-37 recite: that error condition information is a conditional expression indicating a condition for causing no decryption error; that the conditional expression is represented as $2 \cdot p \cdot d + 2df - 1 < q/2$,with respect to a non-negative integer p, a non-negative integer q, a non-negative integer d, and a non-negative integer df; and that the non-negative integer df specifies a number of coefficients in a private key polynomial f whose coefficient values equal to 1. Applicants respectfully submit that any combination of Hoffstein and Irvin fails to disclose, suggest, or otherwise render obvious the above-noted features of claims 18-37 for reasons similar to those discussed above with respect to claim 1. Therefore, claims 18-37 are patentable over any combination of Hoffstein and Irvin.

II. Conclusion

In view of the foregoing remarks, Applicants respectfully submit that claims 1-14 and 17-37 are clearly in condition for allowance. An early notice thereof is earnestly solicited.

If, after reviewing the above, the Examiner believes that there are any issues remaining which must be resolved before the application can be passed to issue, it is respectfully requested that the Examiner contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Masato YAMAMICHI et al.

/Stephen W. Kopchik/
2010.12.17 10:34:17 -05'00'

By _____
Stephen W. Kopchik
Registration No. 61,215
Attorney for Applicants

SWK
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
December 17, 2010